UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,543	04/23/2007	Ofir Arkin	ARKIN2	3198

1444 7590 06/16/2010

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
SEKUL, MARIA LYNN	

ART UNIT	PAPER NUMBER
2461	

MAIL DATE	DELIVERY MODE
06/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/580,543	ARKIN, OFIR	
	Examiner	Art Unit	
	MARIA SEKUL	2461	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-75* is/are pending in the application.

4a) Of the above claim(s) *48 and 65* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47,49-64 and 66-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 May 2006* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/04/2010 has been entered.

Status of Claims

1. **Claims 47, 49-64, 66-75** are pending. **Claims 48 and 65** are currently cancelled. **Claims 74 and 75** are newly added. **Claims 1-46** were previously cancelled.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. **Claim 47, 49-50, 52-64, 66, 68-75** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Satish et al. (US Patent No. 7506056)** ("Satish") in view of **Wu (US Patent No. 5,185,860)**.

As to **claims 47, 64, 72 and 73**, Satish discloses a method, network collector, program storage device and computer program product for "enabling detection of data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to said one or more detected nodes, to yield detected data, thereby enabling detection of said data passively (**Fig. 1**; monitoring server 112A may detect when a node **110** attempts to join the system **100** and may create an initial configuration fingerprint for the node, **col. 3, lines 46-50**; monitoring server **112A** may monitor network traffic of the nodes 110 to determine selected aspects of their configurations, **col. 3, lines 58-63**);

"analyzing said detected data and data relating to said communication network to identify at least one of identified information and missing information (network traffic for the node may be passively monitored, i.e. by the monitoring server **112A** which intercepts network messages generated by the node **110** and inspects ("analyzes") the network messages ("detected data") in order to determine various aspects of the configuration of the node, **col. 7, lines 1-7**);

"said data relating to said communication network comprising node identification data" (because monitoring server **112A** detects when a node **110** attempts to join the system, **col. 3, lines 46-49**, it is implicit that because the monitoring server can

determine when a node is joining the system or is already in the system that the monitoring server has information regarding which nodes are known or not known to the system ("node identification data");

"said identified information comprising at least one of nodal information relating to the one or more detected nodes and nodal information relating to said communication network" (monitoring server **112A** determines aspects of the configuration of the node by intercepting and inspecting network messages which include information specifying, e.g. browser application or operating system in use on the node, **col. 7, line 4-12**); and

"storing at least a part of the identified information on a storage device comprising a computer readable medium accessible thereto" (various configuration fingerprints for the nodes **110** may be stored, e.g. in a database **118, Fig. 1A**).

Satish does not explicitly disclose:

"said missing information comprising at least one of missing information regarding at least one of said one or more detected nodes and missing information regarding said communication network"; and

"if said missing information is identified, then querying at least one of one or more nodes operating in said communication network for said missing information provided at least partially from said storage device, giving rise to the queried nodes, thereby collecting said missing information actively".

Satish teaches the monitoring server **112A** may determine aspects of the node's configuration by actively communicating with the node, e.g. monitoring server **112A** may query network software executing on the node **110** to determine which TCP/IP network

ports are active on the node (**col. 7, lines 16-37**). The configuration generation software **150** as part of the monitoring server **112A** (see **Fig. 2**) *may also, or may alternatively*, monitor network traffic in order to passively determine aspects of the nodes' configuration (**col. 5, lines 18-28**). As such, Satish teaches collection of node information passively and/or actively by querying, and further, any of the various aspects of the nodes' configuration that monitoring server wants to collect may be considered "missing information".

Wu teaches discovering information about each node to build a database about the network (**col. 5, lines 37-41**). As noted in the Background of Wu, a network probe determines nodes on a network (**col. 1, lines 54-58**). A network probe **224** (**Fig. 2**) locates defective nodes and assists in repairing those nodes; the discovery system may obtain information from the node to assist in discovering other nodes (**col. 5, lines 25-33**). For each node in the list of nodes, the discovery module of **Fig. 6** may send a ping to determine, e.g. the status of the node and whether it has changed since the last information was obtained (**Fig. 8**). The information queried is information not in the database or is not current after a certain time interval ("missing data").

Wu and Satish are analogous in the art because they pertain to obtaining node information of the network. It would have been obvious to one skilled in the art at the time the invention was made to use the known technique of querying a node for additional information about the node if the information is not currently known to improve the similar method of Satish in the same way, where Satish has initial node

information collected passively and Wu has an initial list of nodes from some source, e.g. a network probe.

As to **claims 49 and 66**, Satish in view of Wu discloses all of claims 47 and 64, respectively.

Satish further discloses "nodal information comprises operating system information relating to operating systems operating on the one or more nodes" (monitoring server **112A** may intercept network messages which may include information specifying an operating system version being executed by the node **110**, **Fig. 1A; col. 7, lines 1-10**).

As to **claim 50**, Satish in view of Wu discloses all of claim 49.

Satish further discloses "the nodes are included in at least one of the following: detected nodes and queried nodes" (monitoring server **112A** may determine a node's configuration passively by intercepting and inspecting ("detected node"), **col. 7, lines 1-7**) or by actively communicating with the node via queries ("queried node"), **col. 7, lines 16-24**).

As to **claims 52 and 68**, Satish in view of Wu discloses all of claims 49 and 66, respectively.

Satish further discloses "receiving data corresponding to data conveyed by a detected node, to yield received data (network traffic for the node may be passively monitored, i.e. by the monitoring server **112A** which intercepts network messages ("receiving data") generated by the node **110** ("detected node"), **col. 7, lines 1-7**);

"inspecting said received data for one or more characteristics of a known operating system" (monitoring server **112A** may intercept network messages which may include information specifying an operating system version being executed by the node **110**, **Fig. 1A; col. 7, lines 1-10**); and

"if inspecting said received data reveals that the data conforms with said one or more characteristics, indicating that the known operating system operates on the detected node" (the various configuration fingerprints for the nodes **110** may be stored, e.g. in a database **118**, **Fig. 1A**, **col. 4, lines 6-8**; fingerprints for the node **110** may comprise any kind of information regarding the configuration of the node and may identify various aspects of software configuration of the node, e.g. the node's operating system type, operating system patch level, etc. **col. 8, lines 8-19**).

As to **claims 53 and 69**, Satish in view of Wu discloses all of claims 47 and 64, respectively.

Satish further discloses "the analyzer is configured to analyze nodal information that comprises runtime information relating to running processes" (the network messages may include information specifying a browser application in use on the node, **col. 7, line 7-12**).

As to **claim 54**, Satish in view of Wu disclose all of claim 47.

Satish further teaches "runtime information relating to running processes comprises at least one of the following: information relating to network running processes operating on the detected nodes and information relating to local running processes operating on the detected nodes" (monitoring server **112A** determines

aspects of the configuration of the node by intercepting and inspecting network messages which include information specifying, e.g. browser application or operating system in use on the node, **col. 7, line 4-12**).

As to **claim 55**, Satish in view of Wu discloses all of claim 47.

Satish further discloses "nodal information comprises hardware information relating to hardware components associated with the respective detected nodes" (the network messages may include information specifying various information regarding hardware of the node, **col. 7, line 7-12**, e.g. processor type, amount of free disk space, amount of available RAM, etc., **col. 8, lines 19-22**).

As to **claim 56**, Satish in view of Wu discloses all of claim 47.

Wu further teaches "the nodal information comprises topology information relating to physical topology of the communication network" (the discovery system can query the network probe 224 and use information obtained from the probe to assist in discovering other nodes on the network, **col. 5, lines 29-33**; by obtaining information contained in the two tables, i.e. the IF and IP tables, the discovery system can determine what the other interfaces to which a node is connected, and therefore determine other networks to which the node is connected ("physical topology"), **col. 7, lines 40-49**).

As to **claims 57 and 70**, Satish in view of Wu discloses all of claims 47 and 64, respectively.

Satish further discloses "generating a query message corresponding to the missing information for conveying said query message to one or more nodes to be

queried" (monitoring server **112A** determines aspects of the node's configuration by actively communicating with the node **110**, e.g. querying network software executing on the node **110**, **col. 7, lines 16-24**; as stated previously, it is implicit that information being queried is "missing data", particularly during reassessment for a node when subsequent configuration fingerprinting is performed after the node has already joined, **col. 8, line 64-col. 9, line 4**); and

conveying the query message to said one or more nodes, giving rise to the queried nodes (monitoring server **112A** actively communicates with the node **110**, e.g. querying network software executing on the node **110**, **col. 7, lines 16-24**).

As to **claims 58 and 71**, Satish in view of Wu discloses all of claims 57 and 70, respectively.

Satish further discloses "receiving at least one response that corresponds to the query message" (monitoring server **112A** determines aspects of the node's configuration by actively communicating with the node **110**, e.g. querying network software executing on the node **110**, **col. 7, lines 16-24**; it is implicit that monitoring server **112A** receives responses to the query message when actively communicating with the node); and

"processing the at least one response to retrieve information corresponding to the missing information" (monitoring server **112A** queries the nodes to determine ("processing"), e.g. TCP/IP network ports active on the node, **col. 7, lines 18-24**).

As to **claim 59**, Satish in view of Wu discloses all of claim 57.

Wu further discloses "the query message is one of the following: an ARP (Address Resolution Protocol) request; an ICMP (Internet Control Message Protocol) echo request; and a TCP-SYN request" (an ICMP message, or ping message, is sent to a node to determine if the node is still active after a time interval has elapsed, **Fig. 9, col. 7, lines 17-28**).

As to **claim 60**, Satish in view of Wu discloses all of claim 57.

Satish further discloses "the generating is done in accordance with a test policy and wherein the test policy is selected from a group of available test policies" (network admission control may be based on both configuration fingerprints and policy information, where policy information is used to determine whether a node's configuration is satisfactory for admission to the network, and different systems/environments may set different network admission criteria ("plurality of test policies"), **col. 5, lines 53-63**; therefore, it is anticipated that the queries will request node information necessary to apply the policy).

As to **claim 61**, Satish in view of Wu discloses all of claim 57.

Satish further discloses "wherein generating is done in accordance with a test policy" (network admission control may be based on both configuration fingerprints and policy information, where policy information is used to determine whether a node's configuration is satisfactory for admission to the network, and different systems/environments may set different network admission criteria ("plurality of policies"), **col. 5, lines 53-63**; therefore, it is anticipated that the queries will request node information necessary to apply the policy); and

"wherein the test policy is selected in accordance with a statistical computation" (configuration fingerprints are analyzed over time to detect trends indicating, e.g. security threats, **col. 9, lines 16-33**; it is anticipated that the trend being monitored determines the type of information to be collected from the node).

As to **claim 62**, Satish in view of Wu discloses all of claim 57.

Satish further disclose "missing information relates to at least one running process operating on respective queried nodes" (monitoring server **112A** determines aspects of the configuration of the node by intercepting and inspecting network messages which include information specifying, e.g. browser application or operating system in use on the node, **col. 7, line 4-12**; monitoring server may also actively communicate with the node via standard software, e.g. operating system or networking software, **col. 7, lines 30-37**; therefore, it is anticipated that during subsequent configuration fingerprinting of a node, e.g. after a certain time interval, the node may be queried to gather node information rather than waiting for passive detection).

As to **claim 63**, Satish in view of Wu discloses all of claim 57.

Satish further discloses "the detected nodes comprise at least one queried node, and the data conveyed by detected nodes includes at least one response that corresponds to the query message" (the configuration generation software **150** as part of the monitoring server **112A** (see **Fig. 2**) *may also, or may alternatively*, monitor network traffic in order to passively determine aspects of the nodes' configuration (**col. 5, lines 18-28**), and where the subsequent configuration fingerprint indicates the configuration information determined from monitoring the node's network traffic

("detected" or actively communicating with the node **110** ("queried"); as stated, the monitoring server may collect information from node both passively and actively. Therefore, it is implicit that when a query is made to a node from which data has been collected passively, the queried node is also a detected node, and any data conveyed in response to a query is from a detected node.

As to **claims 74 and 75**, Satish in view of Wu discloses the method of claims 47 and 64, respectively.

Satish further discloses "wherein the step of enabling detection is performed in real-time" (network traffic for the node may be passively monitored, and the monitoring server **112A** may intercept network messages generated by the node, **col. 7, lines 1-7**; it is implicit that the monitoring server is enabled in real-time as it intercepts messages generated by the node as they are being sent).

4. **Claims 51 and 67** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Satish et al. (US Patent No. 7506056)** ("Satish") in view of **Wu (US Patent No. 5,185,860)**, and further in view of **Rowland et. al (US PGPub 2003/0212910)** ("Rowland").

As to **claims 51 and 67**, Satish in view of Wu discloses all of claims 49 and 66, respectively.

Satish in view of Wu does not explicitly disclose "detection of the data comprises detecting at least one type of message from a group comprising DHCP (Dynamic Host Configuration Protocol) messages and SYN packets".

Rowland teaches passively monitoring a DHCP server and detecting DHCP packets/messages (**Fig. 4; ¶ 34**).

Rowland and Satish in view of Wu are analogous in the art because they pertain to detecting information about a node. It would have been obvious to use the known technique of detecting DHCP packets/messages as taught in Rowland to improve the similar passive monitoring server as taught in Satish in view of Wu, in the same way.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Norrgard et al. (US PGPub 2005/0105475) - pertaining to topology awareness probes.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARIA SEKUL whose telephone number is (571)270-7636. The examiner can normally be reached on 9 AM to 5:30 PM (ET).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (570) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M.L.S./
Examiner, Art Unit 2461

/Huy D Vu/
Supervisory Patent Examiner, Art Unit 2461